ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

Title and Character of Case:

AIR FORCE INSTITUTE OF TECHNOLGY
MOONLIGHT MAZE

Date Property Acquired: 02/08/1999

Source from which Property Acquired: [redacted] b3 OTHER

Anticipated Disposition:

Acquired By: [redacted] Case Agent: [redacted] b6 b7C

Description of Property: 1B 9

Date Entered

[redacted] b3 OTHER

Barcode: E1394242 Location: ~~ECRAU1~~ ~~BIN1~~ ~~S4~~ 02/08/1999

ECR/4/4

FILE COPY

Case Number: 288-CI-68562 - 1B(9)
Owning Office: SAN ANTONIO

RDW/BB

288-CI-68562-109

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-03-2012

Title and Character of Case:

AIR FORCE INSTITUTE OF TECHNOLGY
-

Date Property Acquired: Source from which Property Acquired:

09/25/1998

[redacted] EIU

CHARLESTON IL

b6
b7C

Anticipated Disposition: Acquired By: Case Agent:

[redacted]

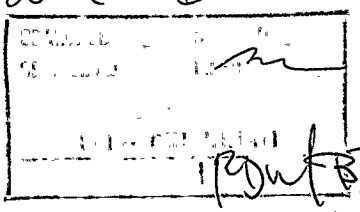
Description of Property: Date Entered

1D 1

TAPE #14058
1 8MM SONY DATA CARTRIDGE
VOLUNTEERED

Barcode: E1474422 Location: ELSUR1 CAB4 S3 10/11/1998

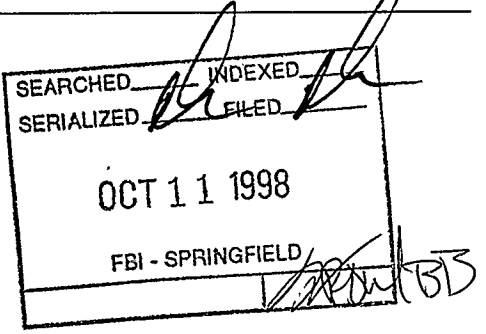
288-CI-68562-131



Case Number: (U) 288-CI-68562 (S) -1D1
Owning Office: SPRINGFIELD

~~SECRET~~

Tape 14058



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

Title and Character of Case:

AIR FORCE INSTITUTE OF TECHNOLGY
MOONLIGHT MAZE

Date Property Acquired: Source from which Property Acquired:

[redacted] AUBURN UNIVERSITY

03/15/1999

b6
b7C

Anticipated Disposition: Acquired By: Case Agent:

[redacted]

Description of Property: Date Entered

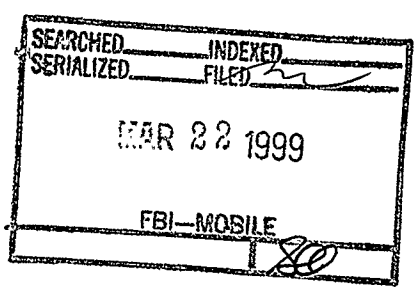
1B 15

ONE(1) SONY 8MM DATA CARTRIDGE

Barcode: E1182456 Location: ECR CAB8 S2 03/18/1999

Case Number: 288-CI-68562 1B15
Owning Office: MOBILE

FILE COPY



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

Title and Character of Case:

AIR FORCE INSTITUTE OF TECHNOLGY
MOONLIGHT MAZE

Date Property Acquired: Source from which Property Acquired:

[redacted] PEN REGISTER [redacted] b3

03/12/1999

Anticipated Disposition: Acquired By: Case Agent:

[redacted] b6 b7C

Description of Property: Date Entered

1B 14

[redacted] PEN b3

REGISTER [redacted]

Barcode: E1663896 Location: 03/17/1999

Case Number: 288-CI-68562-1B14
Owning Office: PHILADELPHIA

[redacted] b6 b7C

Secret

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

FBI FACSIMILE

COVERSHEET

PRECEDENCE

- Immediate
- Priority
- ~~Routine~~

CLASSIFICATION

- Top Secret
- Secret
- Confidential
- Sensitive
- X Unclassified

Time Transmitted
Sender's Initials
Number of Pages 7
(including cover sheet)

To Cincinnati
Name of Office

Date 7/17/98

Facsimile Number 513 562 5648 5838

Attn: SSA [redacted] J
Name Room Telephone

From: NIPC CIU
Name of Office

Subject: Unsub; University of Cin - Victim
Wright-Patterson Air Force Base - Victim
June 1, 1998 to July 9, 1998
CFTA - Intrusion

b6
b7C

Special Handling Instructions: FYI

Originator's Name [redacted] Telephone: [redacted]

Originator's Facsimile Number: 202 324-0311

Approved: ✓

Referral/Consult

Brief Description of Communication Faxed: [redacted]

Secret

JUL 17 1998

CINNATI

b6
b7C

FD-448 (Rev. 6-2-97)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

FBI FACSIMILE

COVER SHEET

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☐ Routine

CLASSIFICATION

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential
- ☐ Sensitive
- ☐ Unclassified

Time Transmitted: 3:30
Sender's Initials: bce
Number of Pages: 26
(including cover sheet)

To: FBIHQ NIPC. Date: 7/14/98
Name of Office

Facsimile Number: 202 324-0311

Attn: UC [redacted]
Name Room Telephone

288/RW/SPK
W/N: NATL SEC PROBLEM OF ASSISTENCE BY UC STUDENT
: COORD 051 - WILL NEED INTERVIEW OF ATEMA ACCOUNT ROMANIAN STUDENT.
: EC TO OPEN 288 [redacted] COMPUTER CONTACTS.
: FORM 801- [redacted] ONE 288.0 PER DO

From: CINCINNATI
Name of Office

Subject: OSI COMPUTER CASE AT WPAFB

Special Handling Instructions:

Originator's Name: SSA [redacted] Telephone: [redacted]

Originator's Facsimile Number: 513 562-5650

Approved: RW

Brief Description of Communication Faxed:

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

FD-801 (Rev. 7-15-97)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/15/1998

To: Director, FBI **Attn:** Computer Investigations Unit,CIOS, NIPC, Rm.11887

From: SAC, Cincinnati

Approved By: [redacted]

Drafted By: [redacted]

b6
b7C

Case ID #: 288-CI-0

Title: Subject: UNSUB;
Victim: USAF-Cataloging and Standardization
Type: Intrustion
Date: 6/2/98

SUBMISSION: X Initial ☐ Supplemental ☐ Closed

CASE OPENED: ___/___/___

CASE CLOSED: ___/___/___
☐ No action due to state/local prosecution
(Name/Number_____)
☐ USA declination
☐ Referred to Another Federal Agency
(Name/Number:_____)
☐ Placed in unaddressed work
☐ Closed administratively
☐ Conviction

8/12/98 [redacted] 8/14/98

b6
b7C

COORDINATION: FBI Field Office IP SA [redacted] (LRA)
Government Agency AFOSI Detachment 101 WPAFB, Dayton, OH
Private Corporation

Company name/Government agency: USAF
Address/location: Federal Center, Battle Creek, MI

Purpose of System: 1) Dracula; e-mail; back up DNS 2)Hyde; Data base server
Highest classification of information stored in system: Unclassified

288-CI-68562-3
288-CI-0-38

SEARCHED ___ INDEXED ___
SERIALIZED ___ FILED ___
JUN 17 1998
FBI – CINCINNATI

7/31/98
Transfer to 288-CI-68525 68562

167CLQ03.OTH

To: Director, FBI From: SAC,
Re: 288- , Date

System Data:

Hardware/configuration (CPU):_1) SunSpare 20 2) SunSpare 1000_____
Operating System: ___Solaris 2.4_____
Software: ___E-mail exchanger; Unify_____

Security Features:

Security Software Installed: ☐ yes (identify _____) **X** no
Logon Warning Banner: **X** yes ☐ no

INTRUSION INFORMATION

Access for intrusion: ☐ Internet connection ☐ dial-up number ☐ LAN (insider)
If Internet: Internet address:
Network name:

b7E

Method:

Technique(s) used in intrusion: _____ (list provided)

Path of intrusion:

addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject:

Age: _____ Race: _____
Sex: _____ Education: _____
Alias(s): _____ Motive: _____
Group Affiliation: _____
Employer: _____
Known Accomplices: _____
Equipment used:
Hardware/configuration (CPU):_____
Operating System: _____
Software: _____

Impact:

Compromise of classified information: ☐ yes **X** no
Estimated number of computers affected: ___2_____
Estimated dollar loss to date: ___Unknown_____

To: Director, FBI From: SAC,
Re: 288- , Date

Category of Crime:

Impairment:
- ☐ Malicious code inserted
- ☐ Denial of service
- ☐ Destruction of information/software
- ☐ Modification of information/software

Theft of Information:
- ☐ Classified information compromised
- ☐ Unclassified information compromised
- ☐ Passwords obtained
- ☐ Computer processing time obtained
- ☐ Telephone services obtained
- ☐ Application software obtained
- ☐ Operating software obtained

Intrusion:
- **X** Unauthorized access Stat D
- ☐ Exceeding authorized access

REMARKS

♦♦

(01/26/1998)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/10/1998

To: National Security **Attn:** NIPC-CIU, Room 11887;
SSA [redacted]

From: Cincinnati
Squad 4
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562 - (Pending) 4

Title: (U) ~~(S)~~ UNSUB(S);
UNITED STATES AIR FORCE
INSTITUTE OF TECHNOLOGY,
HACKING ATTACK ON: [redacted] b7E

Synopsis: (U) ~~(S)~~ Preliminary information and case summary concerning captioned matter.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

[redacted]

(U) Administrative: Referenced enclosures serve as a means to furnish NSD, NIPC-CIU, a more detailed synopsis of captioned matter.

[redacted] Referral/Consult

~~SECRET~~

288-CI-68562-4

Serialized [redacted]
Indexed [redacted]
Filed [redacted]

2223B01EC

TDW/BB

To: National Security From: Cincinnati
Re: (U) (S) 288-CI-68562, 08/10/1998

[redacted] Detective, UC Department of Police, telephone: [redacted]

[redacted] Systems Engineer, UC College of Engineering, telephone: [redacted] b6 b7C

(U) (S) On 08/06/1998 SSA [redacted] Squad 4 Supervisor, and SA [redacted] case Agent, attended a meeting at WPAFB to discuss the mission and direction of captioned matter.

(U) [redacted]

Referral/Consult

(U) [redacted]

(S) The following investigative steps/leads were discussed:

1. NSD/NIPC will pursue the possibility of obtaining a Title III [redacted] b3

[redacted]

[redacted]

Referral/Consult

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

[redacted]

[redacted] shows [redacted]
DOB [redacted] arrived on [redacted] on a F-1 (student) visa.

LEXIS/NEXIS shows current address [redacted]
Previous addresses [redacted]

b6
b7C
b7E

LEADS shows [redacted]
with a current [redacted] driver's license [redacted] issued
[redacted] expiring [redacted] is described as [redacted]

That's all I found.

[redacted]

288-CI-68562-5

SEARCHED
SERIALIZED
INDEXED
FILED

AUG 12 1998

[redacted]

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

FD-759 (Rev. 5-25-95)

Date: 7/31/98

To: Director, FBI ( )
Attn: CID, DIPC-CTU Section

From: SAC, CINCINNATI (288-CI-68502) (P)

For FBI Field Office use only
CM#:

Title:
UNSUB(S);
UCAP
INSTITUTE OF TECHNOLOGY,
HACKING ATTACK ON

Notification of SAC Authority Granted for Use of CONSENSUAL Monitoring Equipment
(Check only ONE)
- ☒ Routine Use
- ☐ Emergency Use-Sensitive Circumstances (cannot exceed 30 days & may be extended only by FBIHQ).

b7E

This form must be typewritten & submitted within 10 working days of the date authority is granted as shown in Item 5 below.

1. Reason for Proposed Use: (Check)
☐ Corroborate Testimony ☐ Protect Consenting Party ☐ Protect Government Property ☒ Collect Evidence
☐ Other (Specify)

2. Type of Equipment: (Check)
☐ Transmitter/Receiver ☐ Concealed Recorder
☐ CCTV/Audio & Video ☐ CCTV Video only
☐ Microphone ☐ Telephone
☒ Other (Specify) Network Monitor

3. Consenting Party (Identify ONLY on Field Office Copy)
☒ Nonconfidential Party
☐ Confidential Source
☐ Cooperative Witness

4. Interceptee(s): (Include Title if Public Official)
University of Cincinnati, College of Engineering & Computer Science
& others as yet unknown.

5. Duration of proposed use:
Authorized On:
☒ For the duration of investigation
☐ For 30 days (Emergency NTCM usage)
Expiring On:

6. Equipment Concealed:
☐ In a Motel Rm. ☐ In a Telephone
☐ In a Residence ☐ On a Person
☐ In a Vehicle
☐ Other (Specify) Secured Network Room

7. City & State where Equipment will be used: Cincinnati, Ohio

8. The following mandatory requirements have been met:
☒ Consenting party has agreed to testify;
☒ Consenting party has executed a consent form; &
☒ Recording/transmitting device will be activated only when consenting party is present.

9. Government Attorney in judicial district where monitoring and/or recording will take place has been contacted; foresees no entrapment; & concurs in the use of the technique.
☒ Yes ☐ No Date of Contact: 7/17/98
Identity of Gov't Atty: AUSA [redacted] b6 b7C
Judicial District: Southern District of Ohio

10. Violation(s): Title(s) 18 Sec(s) 1030 USC

11. DOJ notification required ☐ Yes ☒ No. If "Yes" check reason below:
NOTE: Requests for Routine NTCM usage involving any of the 7 sensitive circumstances requires a teletype to HQ prepared in the format described in the MIOG, Part II, Section 10-10.3 (8). Request for Emergency NTCM usage involving Item 6 below requires immediate contact with the FBIHQ substantive desk for DOJ approval. The 7 sensitive circumstances do not apply to the use of CCTV video only.
1. ☐ Interception relates to an investigation of a member of Congress; a Federal Judge; a member of the Executive Branch at Executive Level IV or above; or a person who has served in such capacity within the previous 2 years.
2. ☐ Interception relates to an investigation of any public official and the offense investigated is one involving bribery; conflict of interest; or extortion relating to the performance of his/her official duties.
3. ☐ Interception relates to an investigation of a Federal law enforcement official.
4. ☐ Consenting/nonconsenting party is a member of the diplomatic corps of a foreign country.
5. ☐ Consenting/nonconsenting party is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.
6. ☐ **Consenting/nonconsenting party is in the custody of the Bureau of Prisons or the U.S. Marshals Service.**
7. ☐ Attorney General; Deputy Attorney General; Associate Attorney General; Assistant Attorney General for the Criminal Division; or the U.S. Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent for making a consensual interception in a specific investigation.

12. Synopsis of Case: (Attach additional page if necessary)
Please see attached.

13. Justification statement necessitating emergency authorization:
☐ Emergency 30 day authorization granted due to imminent need (within 48 hours) for use of consensual monitoring device(s), which precluded the handling of this request in the usual manner.
☐ Other (Attach Additional Page to Specify)

Field Approval
14. CDC (If Sensitive Circumstances Exist)
Signature Date:
15. SAC
Signature [signature] Date: 7/31/98

FBIHQ Approval
16. Unit Chief (If Sensitive Circumstances Exist)
Signature Date:

1-Government Attorney's Office

Attn:

COPY 4

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

Referral/Consult

Background:

[redacted]

b. Governing Statutes:

(U) Title 18, United States Code (USC), Section 1030, Fraud and Related Activity in Connection with Computers

MISSION:

(U) ~~(S)~~ The primary mission of this operation will be to identify modus operandi, tradecraft and tools being utilized by this hacker. If possible, determine if the hacker is associated with a Foreign Intelligence Service and the extent of the FIS involvement and direction in his/her activity. If this is a FIS operation it would also provide extensive insight in to the conduct of FIS and their capabilities in attacking our information systems. Through these efforts we will identify the vulnerabilities which allowed this individual to gain access to the computer systems, thereby being able to anticipate and develop countermeasures to prevent this from taking place in the future. This would not only apply to the AFIT/WPAFB systems but to computer systems throughout the Department of Defense.

(U) A secondary objective of this investigation is to reduce, through prosecution, the hacking activities against military, commercial and private computer and network systems.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

FD-759 (Rev. 5-25-95)

To: Director, FBI ( )
Attn: CID, NIPC-CIU Section

From: SAC, CINCINNATI (288-CI-68562) (P)

Date: 7/31/98

For FBI Field Office use only
CM#:

Title: UNSUB(S);
USAF
INSTITUTE OF TECHNOLOGY
HACKING ATTACK ON
[redacted]

Notification of SAC Authority Granted for Use of CONSENSUAL Monitoring Equipment
(Check only ONE)
☒ **Routine Use**
☐ **Emergency Use-Sensitive Circumstances (cannot exceed 30 days & may be extended only by FBIHQ).**

b7E

This form must be typewritten & submitted within 10 working days of the date authority is granted as shown in Item 5 below.

1. Reason for Proposed Use: (Check)
☐ Corroborate Testimony ☐ Protect Consenting Party ☐ Protect Government Property ☒ Collect Evidence
☐ Other (Specify)

2. Type of Equipment: (Check)
☐ Transmitter/Receiver ☐ Concealed Recorder
☐ CCTV/Audio & Video ☐ CCTV Video only
☐ Microphone ☐ Telephone
☒ Other (Specify) Network Monitor

3. Consenting Party (Identify ONLY on Field Office Copy)
☒ Nonconfidential Party
☐ Confidential Source
☐ Cooperative Witness

4. Interceptee(s): (Include Title if Public Official)
Wright State University, College of Engineering & Computer Science
& others as yet unknown.

5. Duration of proposed use:
Authorized On: _____
☒ For the duration of investigation
☐ For 30 days (Emergency NTCM usage)
Expiring On: _____

6. Equipment Concealed:
☐ In a Motel Rm. ☐ In a Telephone
☐ In a Residence ☐ On a Person
☐ In a Vehicle
☒ Other (Specify) Secured Network Recer

7. City & State where Equipment will be used: Dayton, Ohio

8. The following mandatory requirements have been met:
☒ Consenting party has agreed to testify;
☒ Consenting party has executed a consent form; &
☒ Recording/transmitting device will be activated only when consenting party is present.

9. Government Attorney in judicial district where monitoring and/or recording will take place has been contacted; foresees no entrapment; & concurs in the use of the technique.
☒ Yes ☐ No Date of Contact: 8/17/98
Identity of Gov't Atty: AUSA [redacted]
Judicial District: Southern District of Ohio

b6
b7C

10. Violation(s): Title(s) 18 Sec(s) 1030 USC

11. DOJ notification required ☐ Yes ☒ No. If "Yes" check reason below:
NOTE: Requests for Routine NTCM usage involving any of the 7 sensitive circumstances requires a teletype to HQ prepared in the format described in the MIOG, Part II, Section 10-10.3 (8). Request for Emergency NTCM usage involving Item 6 below requires immediate contact with the FBIHQ substantive desk for DOJ approval. The 7 sensitive circumstances do not apply to the use of CCTV video only.
1. ☐ Interception relates to an investigation of a member of Congress; a Federal Judge; a member of the Executive Branch at Executive Level IV or above; or a person who has served in such capacity within the previous 2 years.
2. ☐ Interception relates to an investigation of any public official and the offense investigated is one involving bribery; conflict of interest; or extortion relating to the performance of his/her official duties.
3. ☐ Interception relates to an investigation of a Federal law enforcement official.
4. ☐ Consenting/nonconsenting party is a member of the diplomatic corps of a foreign country.
5. ☐ Consenting/nonconsenting party is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.
6. ☐ **Consenting/nonconsenting party is in the custody of the Bureau of Prisons or the U.S. Marshals Service.**
7. ☐ Attorney General; Deputy Attorney General; Associate Attorney General; Assistant Attorney General for the Criminal Division; or the U.S. Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent for making a consensual interception in a specific investigation.

12. Synopsis of Case: (Attach additional page if necessary)

Please see attached.

13. Justification statement necessitating emergency authorization:
☐ Emergency 30 day authorization granted due to imminent need (within 48 hours) for use of consensual monitoring device(s), which precluded the handling of this request in the usual manner.
☐ Other (Attach Additional Page to Specify)

Field Approval
14. CDC (If Sensitive Circumstances Exist)
Signature _____ Date: _____
15. SAC
Signature [redacted] Date: [redacted]

FBIHQ Approval
16. Unit Chief (If Sensitive Circumstances Exist)
Signature _____ Date: _____

1-Government Attorney's Office

Attn: _____

COPY 4

FD-302 (Rev. 10-6-95)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/12/98

employed at provided witness accounts of hacking related activity at his business location. can be contacted at his work, Also present during this interview/meeting were At the outset of the interview was provided with a certified copy of United States District Court Order, For the Southern District of Ohio, Western Division, Number 98-235 E, filed 08/07/1998, signed by United States Magistrate Judge, Timothy S. Hogan, Cincinnati, Ohio.

b6
b7C

advised, that on he was contacted by in reference to a possible intruder (hacker) who appeared to have broken into one of computer systems. are located in the same building. The IP of the computer system in question is and this IP address resolves to cartman.aticorp.org.

b6
b7C
b7E

advised that while doing routine network duties he utilized

Due to this unknown connection to their system, started then attempted to contact AFCERT, CERT, WPAFB, and the FBI. was only able to reach WPAFB and made contact with a and a at AFCERT.

b6
b7C
b7E

no hard copy rec'd

Investigation on 08/07/98 at North Charleston, SC

File # 288-CI-68562-6 Date dictated 08/12/98

AFOSI Agent

by SA

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted]

b6
b7C
b7E

[redacted] is assigned to [redacted] AFRL/IFTA, Building 620, Room N3F22, 2241 Avionics Circle, Wright-Patterson AFB, OH 45433-7334, Phone: [redacted] E-mail: [redacted] explained [redacted] They share a working

b6
b7C

relation in their professional dealings. [redacted] did not provide a broad background on what a [redacted] is or does. b6 b7C

[redacted] is assigned to [redacted] ATI Corp., 7611 Barclay Ave., North Charleston, SC 29418, Phone: [redacted] E-mail: [redacted]

[redacted]

b6
b7C
b7E

[redacted]

b6
b7C
b7E

[redacted]

b3
b6
b7C
OTHER Sealed Court Documents

(01/26/1998)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/13/1998

To: Cincinnati **Attn:** SA [redacted]

From: Columbia
Charleston Resident Agency
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288-CI-68562 (Pending)

Title: Unknown Subject;
Wright-Patterson Air Force Base - Victim;
CITA - THEFT

Synopsis: Lead to interview officials at South Carolina Research Authority (SCRA) [redacted]

Administrative: [redacted] The results of the interview of [redacted] are set forth in the enclosed FD-302. The items provided by [redacted] during the interview were furnished in duplicate. The originals of the items were received by the FBI and a receipt was provided to [redacted] for the items. The original items received and the receipt are also enclosed to this EC. The copy of the items provided by [redacted] was made available to AFOSI.

b3
b6
b7C
OTHER Sealed Court Documents

Enclosures: Enclosed for CI is the original and two copies of an FD-302 [redacted] interview which was jointly conducted by the FBI and AFOSI.

Also enclosed for CI are the following:

1. A 1-A containing the original receipt provided to SCRA.

[redacted]

no hard copy rec'd yet

288-CI-68562-7

b3
OTHER Seal Court Documents

[redacted]

Details: [redacted]

[redacted]

b7E

. Columbia Division, Charleston RA, is taking no further action regarding this investigation, unless requested to do so by OO.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/05/1998

[redacted] white male, [redacted] College of Engineering, 628 Engineering Research Center, University of Cincinnati, Cincinnati, Ohio 45221, telephone number [redacted] was advised of the identity of the interviewing Agent and the purpose of the interview.

[redacted] advised that he had the authority to monitor the activities of the computers located in the Engineering Research Center. [redacted] signed an FD-472, authorizing the Federal Bureau of Investigation to initiate the monitoring of these computers.

[redacted] provided a list of the Transmission Control Protocol/Internet Protocol (TCP/IP) addresses and fully qualified domain names for the computers in the Engineering Research Center. [redacted] also advised that all of these computers contained the appropriate banners.

b6
b7C

Investigation on 07/31/1998 at Cincinnati, Ohio

File # 288-CI-68562 - 8 Date dictated 08/05/1998

by SA [redacted] mwd

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

RDW/BB

FD-472 (Rev. 1-9-92)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

July 31, 1998
(Date)

University of Cincinnati, Ohio
(Location)

I, [redacted] of

University of Cincinnati, Cincinnati, Ohio, hereby
(Address)

b6
b7C

authorize Special Agents [redacted] and

[redacted], of the Federal Bureau of Investigation, United States Department of Justice, to:

☒ install a recording device on any telephone utilized by me for the purpose of recording any telephone conversation(s) I may have with

_____ and others as yet unknown
(Name of Subject(s))

on or about _____ and continuing thereafter.
(Date)

I understand that I must be a party to any conversation in order to record that conversation. I therefore agree not to leave the recording equipment unattended or take any action which is likely to result in the recording of conversations to which I am not a party.

and/or to:

☐ install a Trap and Trace device in conjunction with the appropriate provider(s) of electronic or wire communications service and/or long distance carrier for the purpose of identifying telephone numbers from which incoming calls are placed to telephone number _____
located at _____
which is used by me.

Initiate the monitoring of the computers in the University of Cincinnati Engineering Department computer lab. I have the authority to monitor these computers.

I have given this written permission to the above-named Special Agents voluntarily, and without threats or promises of any kind.

[redacted]
(Signature)

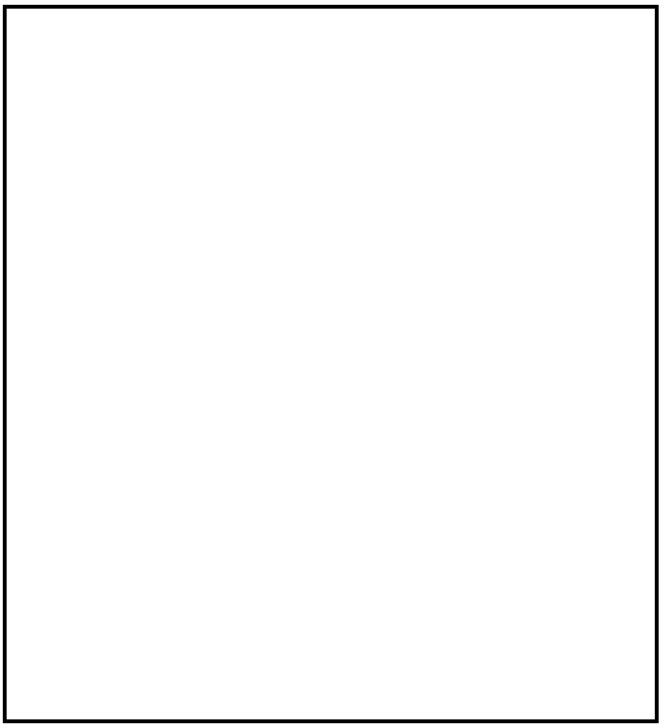
b6
b7C

Witnessess:

[redacted]

FBI/DOJ

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio



b6
b7C

FAX TO (202) 324-0311

FROM SA [redacted]
Cincinnati, OH

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 08/23/1998

To: National Security **Attn:** NIPC-CIU, Room 11887;
SSA [redacted]

From: Cincinnati
Squad 4
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID # (U) ~~(S)~~ 288-CI-68562 (Pending)

Title (U) ~~(S)~~ UNSUB(S);
UNITED STATES AIR FORCE
INSTITUTE OF TECHNOLOGY,
HACKING ATTACK ON: [redacted] b7E

Synopsis (U) ~~(S)~~ Summary update of captioned matter.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

(U) **Details:** ~~(S)~~ What follows is a brief synopsis of actions accomplished as of 08/21/1998:

[redacted] Referral/Consult

(U) ~~(S)~~ FBI Cincinnati obtains consent to monitor UC's College of Engineering and Computer Science subnet 129.137.41.x utilizing FBI Form FD-472 on July 31, 1998.

[redacted]

~~SECRET~~

288-CI-68562-9

Searched
Serialized
Indexed
Filed

235BB01.EC

(U)

Referral/Consult

(U) (S) On August 21, 1998, [redacted] Engineering Research Facility (ERF), Quantico, Virginia, and [redacted] ERF, visited Cincinnati, Ohio, for the purpose of determining how to expand the network monitoring system at UC.

b6
b7C

(U) (S) Subsequent a meeting with UC staff to include systems engineers and administrators, the following issues were discussed:

(U) (S) There are various end user systems identified as their own system administrators linked to the UC systems. If and

[redacted] b7E

(U) [redacted]

(U) (S) [redacted] learned the following, UC's system network interface utilizes a 10 megabit Ethernet pipe out to the Internet. b6 b7C

(U) (S) In order to monitor UC's College of Engineering and Computer Science subnet, two options exist:

(U) [redacted] b7E

(U) [redacted]

(U) (S) A mutual suggestion was discussed. Inasmuch that SCRA's network has been blocked from all possible angles from UC, WSU, Infinet and WPAFB, the consensus was that SCRA be dropped from further scrutiny due to limited resources and time constraints.

To: National Security From: Cincinnati
Re: (U) (S) 288-CI-68562, 08/23/1998

(U) (S) Cincinnati respectfully requests that FBIHQ coordinate with AFOSI HQ (DOD) to ameliorate legality issues presented on page three of this communication.

(U) (S) Cincinnati Division expects to conduct witness/suspect/victim interviews during the latter part of August, 1998, and the first week of September, 1998.

(U) (S) Investigation continuing at Cincinnati.

♦♦

DATE: 07-06-2012
CLASSIFIED BY 60324/UC/baw/sab/aio
REASON: 1.4 (c)
DECLASSIFY ON: 07-06-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/13/1998

To: Cincinnati **Attn:** SA

From: Cincinnati
Squad 4
Contact: SA

b6
b7C

Approved By:

Drafted By:

Case ID #: ~~(S)~~ (Pending)
(U) ~~(S)~~ 288-CI-68567 (Pending)

b1
b3

1 + 2

Title: (U) ~~(S)~~ UNSUB(S);
United States Air Force
Institute of Technology,
Hacking Attack On:

b7E

~~(S)~~ **Synopsis:**

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

b1
b3
b7E

(U)

Details:

~~(S)~~

~~(S)~~

~~SECRET~~

288-CI-68562-10
288-CI-68567

SEARCHED INDEXED
SERIALIZED FILED
AUG 13 1998
FBI — CINCINNATI

To: Cincinnati From: Cincinnati
Re: (S) 08/13/1998

b1
b3

(S)

(S)

(S)

(U) (S) Lexis/Nexis, and LEADS confirmed portions of the above information and by separate insert added certain details.

b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/31/98

[redacted] was furnished a copy of an Order (Case No. 98 244 E), signed by the Honorable [redacted] U.S. Magistrate Judge, Cincinnati, Ohio, [redacted] b3 b6 b7C

During the late evening of 08/26/1998 and early morning hours of 08/27/1998, [redacted] a pen register and trap and trace device [redacted] b3 b6 b7C

Investigation on 08/26/1998 at Cincinnati, Ohio

File # 288-CI-68562 -13 Date dictated 08/31/1998

by SA [redacted] b6 b7C
SA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

(01/26/1998)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 09/04/1998

To: National Security **Attn:** NIPC-CIU, Room 11887;
SSA [redacted]

Springfield **Attn:** Champaign RA

From: Cincinnati
Squad 4
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID # (U) ~~(S)~~ 288-CI-68562 - (Pending) 15

Title (U) ~~(S)~~ UNSUB(S);
UNITED STATES AIR FORCE
INSTITUTE OF TECHNOLOGY,
HACKING ATTACK ON:
[redacted] b7E X

Synopsis: (U) ~~(S)~~ Lead set for Springfield Division, Champaign RA, [redacted]

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~ b3 OTHER Sealed Court Docum

Enclosures: (U) ~~(S)~~ Enclosed for Springfield Division, Champaign RA [redacted] b6 b7C

Details: (S) For information of Springfield Division, Champaign RA, Cincinnati Division, along with United States Air Force Office of Special Investigations (AFOSI), are jointly investigating intrusions into computers located at Wright-Patterson Air Force Base (WPAFB), Dayton, Ohio. The intrusions appear to be originating in Russia, hopping through University of Cincinnati, then terminating at WPAFB. The intruder has transferred several sensitive, though not classified files, to

~~SECRET~~

288-CI-68562-15

Searched
Serialized
Indexed
Filed

2470301, EC

To: National Security From: Cincinnati
Re: (U) (S) 288-CI-68562, 09/04/1998

Referral/Consult

(U) (S) On 08/26/1998, the intruder was observed making connections to various other sites not previously seen, to include Eastern Illinois University (EIU). At approximately 0403 CDT, August 31, 1998, the intruder connected to ux1.cts.eiu.edu (139.67.8.3) via telnet, and subsequently via File Transfer Protocol (FTP). Cincinnati Division is desirous of obtaining the username which the intruder accessed into EIU's system.

(U) (S) Cincinnati Division appreciates assistance from the Springfield Division, Champaign RA.

To: National Security From: Cincinnati
Re: (U) (S) 288-CI-68562, 09/04/1998

LEAD (s):

Set Lead 1:

b3
b6
b7C
OTHER Sealed Court Docume

SPRINGFIELD

AT CHARLESTON, IL

(U) (S)

♦♦

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-05-2012

~~SECRET~~

Case ID: 288-CI-68562
Serial: 15

Lead 1 Set to: SPRINGFIELD

Total leads set: 1
Total leads not set: 0

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/19/98

white Female, DOB SSAN POB Visa# Telephone: was advised of the identity of the interviewing Agents and the purpose of the interview. voluntarily furnished the following information:

advised she came to Cincinnati under an F-1 visa from She chose to attend because it was one of the few universities that accepted her. She obtained limited funds from an entity from that funds students to study abroad. She is currently a Ph.D. candidate in

b6
b7C

Prior to arriving in the U.S., was employed as a Her duties involved

b6
b7C

From worked as at the Her job entailed

attended and studied at She obtained an M.S. degree in

advised she has no family and/or relatives residing with her She maintains telephonic and e-mail contact with family and friends

b6
b7C

revealed she gave her computer password out to her boyfriend so that he could e-mail messages to her. Her password at that time was She claims she changed her password after only two days because she knew it was wrong to give out her password. Her boyfriend is a She claims not to

Investigation on 09/18/98 at Cincinnati, Ohio

File # 288-CI-68562-116 Date dictated 09/19/98

b6
b7C

by SA
SA

261b 01.302

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

know whether her boyfriend ever served with [redacted] and/or ever held a clearance.

[redacted] affirmed she visited her parents and friends in [redacted] With respect to her long term goals, [redacted] expects to remain at [redacted] for another four to five years to pursue her Ph.D. [redacted] Upon graduation, she would like to work in the U.S. for about one year, provided she can find a host and obtain employment, before returning to [redacted] or some other European country. b6 b7C

[redacted] stated she has never maintained contact with any government officials either in the U.S. or overseas. She has never been tasked by a Foreign Intelligence Officer to operate either covertly or overtly in the U.S. [redacted] advised she would contact the writer if any unusual activity would ever take place concerning her studies [redacted] and her travels abroad [redacted] b6 b7C

[redacted] is currently a [redacted] wherein she receives a stipend to cover tuition and modest living expenses. Her research, though unclassified, involves [redacted]

[redacted] recalled that in [redacted] or so, she was informed by the systems administrator to change her password. She learned that someone unknown had used her password to hack into [redacted] network using her account. She changed her password and never heard back from the systems administrator. b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/14/98

[redacted] DOB [redacted] SSAN [redacted]
[redacted] telephone: [redacted] was advised of the identity of the interviewing Agents and the purpose of the interview. [redacted] voluntarily furnished the following information: b6 b7C

[redacted] recollected that on or about May 15, 1998, he returned from a business trip to Japan. Upon returning to work, he was informed by two co-workers that his Picard account had been hacked into. He learned that the intrusion came from the University of Cincinnati (UC).

[redacted] revealed that his computer usage is minimal. He uses the computer for word processing and e-mail. He has two e-mail accounts; Picard for long distance e-mail and Teamlinks for e-mail within Wright Patterson Air Force Base (WPAFB). b6 b7C

[redacted] advised that as a result of the hacking incident, the computer network systems administrator issued everyone with a new password, based on name and telephone number. Despite this precaution, the account was again hacked. As recently as July, 1998, the systems administrator instructed every user to alter their passwords to make them more difficult to penetrate.

[redacted] relayed that his Picard e-mail contacts are extensive. He stated that in the last year he has received many messages from the U.S. and from numerous countries abroad to include: England, France, Germany, Finland, Russia, Chile, Japan, New Zealand and Australia. The e-mail message from Russia came from [redacted] a reputed well known scientist from [redacted] He believes [redacted] is from [redacted] recalled that [redacted] has traveled to Dayton and/or Columbus, Ohio and San Francisco, California sometime in 1996. [redacted] annually makes numerous requests seeking joint venture projects with WPAFB researchers. WPAFB is precluded from accepting any joint venture projects with [redacted] according to [redacted] added that [redacted] has published numerous articles on titanium aluminite. b6 b7C

[redacted] recollected that he received one e-mail

Investigation on 09/11/98 at Dayton, Ohio

File # 288-CI-68562 -17 Date dictated 09/14/98

by SA [redacted] SA [redacted] (AFOSI) b6 b7C

254 66 01. 302

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

message from a [redacted] who inquired about scientific research.

According to [redacted] his e-mail contacts with U.S. persons and individuals overseas are all researchers and scientists from sundry educational institutes. The e-mail messages concern scientific discussions relating to metallurgy. [redacted] asserted that none of his e-mail contacts appear to be out of the scope of his purview. [redacted] added that none of the e-mail messages requested secret or proprietary information.

b6
b7C

[redacted] revealed he obtained his U.S. citizenship on [redacted] He has a sister and cousins residing in England. He has worked in [redacted] in the past. As a physicist working in the aforementioned countries, he has never held a security clearance. He maintains no foreign government contacts.

FD-302 (Rev. 10-6-95)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/14/98

[redacted] DOB [redacted] SSAN [redacted] [redacted] telephone: [redacted] was advised of the identity of the interviewing Agents and the purpose of the interview. [redacted] voluntarily furnished the following information:

[redacted] recalled that approximately a few months ago she received a telephone call on a Monday from [redacted] (ATI-CORP), inquiring whether or not she was logged on to their system at 3:00 A.M. in the morning. [redacted] responded negatively and from that moment forward they realized that an unknown individual utilized her username and password to break into the SCRA/ATI-CORP computers and then into Wright Patterson Air Force Base (WPAFB), Dayton, Ohio. b6 b7C

[redacted] had an account at SCRA/ATI-Corp for about three years to transfer files and slides relating to the Rapid Prototyping of Application Specific Signal Processing (RASSP) program. She stated that she no longer holds this account since this incident occurred. The account was shut down. She claims that none of this information was classified or sensitive. Her job requires that she review material to ensure that it is cleared for public domain. The information was publicly released/releasable.

[redacted] advised she maintains accounts on elhp and Fleetwood at her office. She also has root password with her system administrator, [redacted] maintains a flyer net account and a sabre account at the University of Dayton (UD). She had an account at the Air Force Institute of Technology (AFIT) but believes it is no longer valid. [redacted] had a temporary account at the University of Cincinnati (UC) for a three day course she attended at UC [redacted] She held one other account at a company called RTI but believes it is no longer open. b6 b7C

[redacted] asserted that her ATI-Corp account was mainly used for education modules and to transfer files through FTP. She occasionally remote shelled to that account. [redacted] recalled that a week prior to this incident, she logged onto the ATI-Corp machine to FTP some files. She believes she logged on from elhp.

Investigation on 09/11/98 at Dayton, Ohio

File # 288-CI-68562-18 Date dictated 09/14/98

by SA [redacted] SA [redacted] (AFOSI) b6 b7C

25466 02.302

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

She FTP'd information from her PC on other occasions.

[redacted] affirmed that she has never given out any of her passwords with the exception of her root password on elhp which [redacted] has access to. b6 b7C

[redacted] revealed that her password [redacted] at ATI-Corp was a combination of upper and lower case letters and symbols which would have been difficult to decipher. [redacted] changed her password to [redacted] per the request of [redacted]

[redacted] added that "the subject probably could have gotten away with it if they wouldn't have logged in at 3:00 A.M. on a Sunday morning."

[redacted] was born in [redacted] the daughter of a [redacted] She has one brother who resides in [redacted] with their mother. Her father is deceased. [redacted] arrived in the U.S. in [redacted] to finish high school in [redacted] where her brother previously resided. She returned to [redacted] to visit her parents and taught English grammar at [redacted] for three months during the summer. b6 b7C

[redacted] was previously married to an active duty U.S. military serviceman. She has been divorced for [redacted] years. She is a U.S. citizen through her previous marriage to a U.S. citizen. [redacted] occasionally travels overseas to visit her family [redacted] Her last trip [redacted] was approximately [redacted] years ago. [redacted] affirmed she has never held a security clearance either in the U.S. or overseas. [redacted] maintains limited contact with friends and family overseas via e-mail.

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-06-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 09/19/1998

To: National Security **Attn:** NIPC-CIU, Room 11887;
SSA [redacted]

From: Cincinnati
Squad 4
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562 (Pending)

Title: CHANGED
(U) ~~(S)~~ MOONLIGHT MAZE

Synopsis (U) ~~(S)~~ Interviews conducted at Cincinnati Division.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

Previous Title (U) ~~(S)~~ Title marked "Changed" to reflect new title as, "MOONLIGHT MAZE." Title previously carried as, "UNSUBS; UNITED STATES AIR FORCE INSTITUTE OF TECHNOLOGY, HACKING ATTACK ON: [redacted] b7E

Enclosures: (U) ~~(S)~~ Enclosed for FBIHQ are three separate copies of FD-302s of interviews conducted by the writer of [redacted] and one Air Force Form 1168 with attached statement of [redacted] b6 b7C

Details: (U) ~~(S)~~ For information of FBIHQ, FBI Cincinnati and United States Air Force, Office of Special Investigations (AFOSI), Wright-Patterson AFB, Dayton, Ohio, conducted four victim/witness interviews. The results of those interviews are enclosed as enclosures for NIPC-CIU, FBIHQ.

(U) ~~(S)~~ Cincinnati Division plans to re-interview [redacted] based on her nervous demeanor and her apparent, less than candid responses concerning her boyfriend who resides in [redacted] computer password at [redacted] will be closely monitored to b6 b7C

~~SECRET~~

288-CI-68562-19

Searched _____
Indexed _____
Filed _____

262BB01.EC

determine whether a change in the subject(s) modus operandi (hacking tools and signature) is detected. A change in the subject(s) hacking activity could explain a nexus between the subject(s) and [redacted] considering her telephonic and e-mail contacts with her boyfriend [redacted] and her recent travels [redacted]

(U) ~~(S)~~ Based on the aforementioned, Cincinnati Division will re-interview the subject with additional probing questions concerning her contacts [redacted] and if deemed appropriate, will consider the use of a polygraph [redacted]

b6
b7C

♦♦

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-06-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 09/28/1998

To: Cincinnati **Attn:** SA [redacted]
Squad 4

From: Springfield
Squad 3/Champaign RA
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562 (Pending) -20

Title: (U) ~~(S)~~ UNSUBS;
UNITED STATES AIR FORCE
INSTITUTE OF TECHNOLOGY;
HACKING ATTACK ON: [redacted] b7E

Synopsis (U) ~~(S)~~ Lead set for Springfield at Charleston, Illinois has been covered.

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 15

Administrative: (U) ~~(S)~~ Re telcall between SA [redacted] and SSA [redacted] on 09/28/1998. b6 b7C

Enclosures: (U) ~~(S)~~ Enclosed for Cincinnati are two copies of computer activity logs.

Package copy: (U) ~~(S)~~ Being forwarded under a separate cover is one 8 mm Data cartridge.

Details: (U) ~~(S)~~ [redacted]

b3
b6
b7C
OTHER Sealed Court Documents [redacted]

~~SECRET~~

Lead covered 9/28/98.

288-CI-68562-20
SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
OCT 6 1998
FBI — CINCINNATI
[redacted] b6 b7C

SE: 27 [illegible]

To: Cincinnati From: Springfield
Re: (U) ~~(S)~~ 288-CI-68562, 09/28/1998

directly. Per telcall between SA [redacted] and SSA [redacted] nothing will be sent directly to the National Security Division for evaluation. Springfield considers this lead covered.
♦♦

b6
b7C

(12/31/1995)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/24/1998

To: Cincinnati **Attn:** [redacted]

From: NSD
NIPC/CIOS/CIU/11719
Contact: SSA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288-CI-68562 (Pending)

Title: UNSUB(S);
UNITED STATES AIR FORCE
INSTITUTE OF TECHNOLOGY - VICTIM;
CITA - COMPUTER INTRUSION;
OO: CINCINNATI

Synopsis: This communication is to forward documents to the original case file. Referral/Consult

Enclosure(s): Two copies of Request For Information letters sent to [redacted] One copy of response from NAVCIRT regarding possible material related to captioned matter.

Details: Enclosed for Cincinnati are copies of documents generated by or directed to the National Infrastructure Protection Center (NIPC) regarding captioned matter. These documents are being forwarded to Cincinnati for inclusion in the original case file.

♦♦

288-CI-68562-21

SEARCHED [redacted]
SERIALIZED [redacted] FILED

[redacted] b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 4, 1998

[redacted]

Dear [redacted] Referral/Consult

This letter is to request information from [redacted] databases and published reports that may be relevant to an ongoing FBI criminal investigation. The investigation centers on a series of intrusions into computer systems located at Wright Patterson Air Force Base. The intrusions appear to originate from a series of Internet service providers located in the Russian Federation. It also appears that the intruder is connecting to the ISPs through a "dial-up" connection, which suggests a local (i.e. Russian) point of origin. The FBI currently possesses no information indicating that the attacker is a U.S. person.

Technical information relevant to this request is provided in the enclosure, which also specifies an operational point of contact in the FBI. As additional technical information becomes available, it will be forwarded to the operational point of contact at [redacted]

The FBI legal contact point for this matter is Assistant General Counsel [redacted] Please do not hesitate to call him if you require additional information. Thank you for your assistance in this matter.

Sincerely,

[redacted]

b6
b7C

Associate General Counsel for National Security Affairs

cc: [redacted]
[redacted] OGC/NIPC

The Wright Patterson Air Force Base (WPAFB), a key educational and research and development base, has documented numerous intrusions into approximately eight of their systems. The attacks primarily come through computers located in the computer lab at the University of Cincinnati. However, attacks have been seen from Wright University, located in Dayton, OH and Aticorp.net located in Charleston, SC. The intrusions into these U.S. systems appears to be originating from a dialup connection to four Internet Service Providers (ISPs) located in Russia. The hacking occurs Monday through Friday, midnight and approximately 9:00 a.m. EDT.

The following are the [redacted] involved:

[redacted] b7E

The following passwords or environment variables have been used during the intrusions:

[redacted] b6 b7C

The following are usernames, software authors or tool names:

[redacted] is the name of [redacted] student whose account is being used at [redacted] Our information indicates she is a non-U.S. person.)

[redacted]

The following files are known to have been taken by the hacker from WPAFB:

[redacted] b7E

NIPC Operational POC is SSA [redacted] b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 3, 1998

[redacted]

Referral/Consult

Dea[redacted]

This letter is to request information from [redacted] databases and published reports that may be relevant to an ongoing FBI criminal investigation. The investigation centers on a series of intrusions into computer systems located at Wright Patterson Air Force Base. The intrusions appear to originate from a series of Internet service providers located in the Russian Federation. It also appears that the intruder is connecting to the ISPs through a "dial-up" connection, which suggests a local (i.e. Russian) point of origin. The FBI currently possesses no information indicating that the attacker is a U.S. person.

Technical information relevant to this request is provided in the enclosure, which also specifies an operational point of contact in the FBI. As additional technical information becomes available, it will be forwarded to the operational point of contact a[redacted]

The FBI legal contact point for this matter is Assistant General Counsel [redacted] Please do not hesitate to call him if you require additional information. Thank you for your assistance in this matter.

Sincerely,

[redacted]

b6
b7C

Associate General Counsel for National Security Affairs

cc: [redacted] OGC/NIPC
NSA

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-06-2012

~~SECRET~~

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 31, 1998

[redacted]

Dear [redacted]

Referral/Consult

This letter is to request [redacted] technical assistance in conjunction with an ongoing FBI criminal investigation. The investigation centers on a series of intrusions into computer systems located at Wright Patterson Air Force Base. The intrusions appear to originate from a (U) series of Internet service providers located in the Russian Federation. It also appears that the intruder is connecting to the ISPs through a "dial-up" connection, which suggests a local (i.e. Russian) point of origin. The FBI currently possesses no information indicating that the attacker is a U.S. person. (S)

The FBI has already made (in an August 21, 1998, letter addressed to Acting General Counsel [redacted] a standard Request for Information in connection with this (U) investigation. The purpose of this letter is to add a technical assistance request so that [redacted] expert personnel can assist the FBI investigators on certain technical questions relating to computer data collected by the FBI. (S)

b6
b7C

The FBI legal contact point for this matter is Assistant General Counsel [redacted] Please do not hesitate to call him if you require additional information. Thank you for your assistance in this matter. (U)

Sincerely,

[redacted]

b6
b7C

Associate General Counsel for National Security Affairs

cc: [redacted]

Referral/Consult

~~Derived From: Multiple Sources~~
~~Declassify on: X1~~

288-CI-68562-22

SEARCHED
SERIALIZED
FBI — CINCINNATI

~~SECRET~~

FD-448 (Rev. 6-2-97)

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-06-2012

FBI FACSIMILE

COVER SHEET

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☒ Routine

CLASSIFICATION

- ☐ Top Secret
- ☒ ~~Secret~~
- ☐ Confidential
- ☐ Sensitive
- ☐ Unclassified

Time Transmitted: 3:53 p.m. MJW
Sender's Initials: MJW
Number of Pages: 2
(including cover sheet)

To: NSA/OGC
Name of Office

Date: 08/31/1998

Facsimile Number: 301-688-6017

Attn: [redacted]
Name Room Telephone

b6
b7C

From: NIPC
Name of Office

Subject: Technical Assistance Request

Special Handling Instructions:

Originator's Name: [redacted]

Telephone: [redacted]

b6
b7C

Originator's Facsimile Number: 202-324-0311

Approved: MJW

Brief Description of Communication Faxed: See Attached

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

FD-448 (Rev. 6-2-97)

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-06-2012

FBI FACSIMILE

COVER SHEET

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☒ Routine

CLASSIFICATION

- ☐ Top Secret
- ☒ Secret
- ☐ Confidential
- ☐ Sensitive
- ☐ Unclassified

Time Transmitted: 3:58 pm.
Sender's Initials: MJW
Number of Pages: 2
(including cover sheet)

To: NSA/[redacted]
Name of Office

Date: 08/31/1998

Facsimile Number: 410-859-4888

Attn: [redacted]
Name Room Telephone

b6
b7C

From: NIPC
Name of Office

Subject: Technical Assistance Request

Special Handling Instructions:

Originator's Name: [redacted] Telephone: [redacted]

b6
b7C

Originator's Facsimile Number: 202-324-0311

Approved: MJW

Brief Description of Communication Faxed: See Attached

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
September 21, 1998

SA [redacted] b6 b7C
USAF Office of Special Investigations
AFOSI Detachment 101
4165 Communications Boulevard, Suite 3
Wright-Patterson Air Force Base, Ohio 45433

To Whom It May Concern:

Upon expiration of AFOSI's Form 52 (Consensual Monitoring) at Wright State University (WSU), FBI Cincinnati will continue monitoring computers at WSU utilizing AFOSI monitoring equipment. Consensual monitoring will be in effect as of the date of this communication to the conclusion of this matter, pursuant to FBI Form FD-759, Notification of SAC authority granted for use of consensual monitoring equipment.

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

By: [redacted] b6 b7C
Supervisory Special Agent

1 - Addressee
1 - Cincinnati (288-CI-68562)

BB:jaw (2)

288-CI-68562-23

Searched
Serialized
Indexed
Filed

264JAW01.OTH

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. 288-CI-68562

550 Main Street, Room 9000
Cincinnati, Ohio 45202
October 6, 1998

DCFL
500 Duncan Avenue, Room 1009
Bolling AFB, DC 20332-6000

SUBJECT: Request for Computer Forensic Media Analysis

1. **COMPLETE SUBJECT TITLE BLOCK INFORMATION:** Wright-Patterson AFB, Ohio, June 1, 1998, Unauthorized access of governmental and civilian computer systems. Violation of Title 18, USC, Section 1030; Fraud and Related Activity in Connection with Computers.

2. **PRIORITY:** This is a Category 1 intrusion on several military systems. This joint investigation is considered one of the highest priority cases within the FBI and AFOSI realms. The analysis of the enclosed tapes is requested immediately by the Department of Justice, Department of Defense, the Federal Bureau of Investigation and AFOSI.

3. **CLASSIFICATION:** This investigation is classified, however the evidence is not.

4. **CO-CASE AGENTS:** SA [redacted], FBI, Cincinnati, Ohio, commercial [redacted] SA [redacted] AFOSI Det 101, WPAFB, Ohio, DSN [redacted] commercial: [redacted] AFOSI Det 101, WPAFB, Ohio, DSN [redacted] commercial: [redacted]

b6
b7C

5. **SYNOPSIS OF THE CASE:** On or about June 1, 1998, WPAFB began detecting intrusions at several Air Force Institute of Technology and Air Force Research Laboratory machines. [redacted] The intrusions originally were detected coming through the University of Cincinnati; however, additional intrusions have been detected at several education sites and numerous Internet Service Providers. The unidentified intruder uses authorized accounts and valid passwords to gain access into the victim systems and then FTP's files, telnets to another system or pop roots. To date, investigative agencies have not been able to detect any sniffer, rootkit or trojanized programming.

b7E

1 - Addressee
1 - Cincinnati (288-CI-68562)
BB:bb (2)

288-CI-68562-26
Searched
Serialized
Indexed
Filed

280BB01, OTH

6. **ITEMS TO BE ANALYZED:**

1. One 3GB Hard Drive, Western Digital Caviar 33100 (University of Wisconsin). **Remarks:** AFOSI Form 96 will be e-mailed to DCFL. The OS and other pertinent information will be on 96.

2. One 4mm Digital Data Storage cartridge, 120M, labeled NVTST/OX, (Wright State University). **Remarks:** Ditto as above.

3. Two 8mm Helical-Scan, HS-8/112 Maxell Data Cartridges [redacted] b7E

SUPPORT REQUESTED:

Extract all system logs, text, document, etc.
Examine file system for modification to operating system software or configuration.
Examine file system for back doors, check for setuid and setgid files.
Examine file system for any sign of a sniffer program.
Extract data from this 4mm/8mm tape and convert to readable format - cut to CD.
Backup hard drives and place backup on a CD, tape or other format.
Analyze for deleted files and restore deleted files, cut findings to CD.
Extract all pertinent text files of a sexual nature.
Extract all trojanized programs or scripts/code programs, cut to CD.
Provide an analysis report and cut all findings to CD.

7. **PERTINENT DATA:** Coordinate with SA [redacted] and HQ AFOSI/XOII with pertinent data. b6 b7C

8. **AUTHORITY:** OSI Form 96 will be sent electronically.

9. **OTHER DOCUMENTS:** The ACISS report is the same as the one sent on the August 26, 1998 request.

10. **INSTRUCTIONS:** Please make five copies and send all copies of the analysis report to HQ AFOSI/XOII. HQ AFOSI/XOII will distribute the analysis accordingly. Please return all evidence to FBI Cincinnati.

11. POC: SA [redacted] AFOSI Detachment 101 at DSN: [redacted] or commercial: [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/26/98

[redacted] Date of Birth (DOB) [redacted] Social Security Account Number (SSAN) [redacted] was advised of the identities of the interviewing Agents and the purpose of the interview. [redacted] voluntarily furnished the following information:

[redacted] identified her boyfriend as [redacted] a white male, DOB [redacted] resides in [redacted] He is a [redacted] who works at a factory [redacted] which utilizes a turbo prop to pump and maintain oil for commercial purposes. [redacted] was unable to identify the factory location and was unable to comment whether the factory has any ties to the [redacted] She recalled that [redacted] has worked there since late [redacted] [redacted] recently informed [redacted] that he is in search of a new job. b6 b7C

[redacted] advised her most recent contact with [redacted] was approximately [redacted] ago via e-mail. [redacted] most recently visited [redacted] She stayed with her family for [redacted] while visiting friends and family.

Prior to enrolling at [redacted] obtained financial assistance from [redacted] a foundation that provides funds for European students to study abroad. [redacted] logged onto [redacted] web site and learned from an advisor the type of research that is conducted at that department. [redacted] liked what [redacted] program had to offer, and as a result, she matriculated at [redacted] is a Ph.D. candidate matriculated in the aforementioned program [redacted] b6 b7C

[redacted] advised her research at [redacted] involves [redacted] In laymen terms, [redacted] utilizes [redacted] According to [redacted] mixed signal design can be used for any and all applications to include military application. [redacted] advised her research at [redacted] is strictly

Investigation on 10/16/98 at Cincinnati, Ohio

File # 288-CI-68562-302 Date dictated 10/29/98

SA [redacted] BB

by [redacted] b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

theoretical research. She does not know who the end user is, of the research she conducts [redacted] Her [redacted]

b6
b7C

[redacted] recalled that during her visit at the U.S. Embassy [redacted] she was interviewed by an embassy employee concerning her request for an exit visa to study abroad. The employee spoke Romanian and English. He asked [redacted] the following questions:

1. Who is funding your trip?
2. How long will you be in the U.S.?
3. Why are you traveling to the U.S.?
4. When will you return?
5. Do you have any family in the U.S.?
6. Will you be working in the U.S.?

[redacted] asserted the interview lasted approximately fifteen minutes. The interviewer was male and was dressed in a suit and tie. The interview was conducted within the confines of the general office space where there was no expectation of privacy. [redacted] affirmed that at no time was she asked, promised, and/or influenced to cooperate with embassy officials and/or other government employees.

b6
b7C

[redacted] stated that she maintains weekly e-mail correspondence with her boyfriend, [redacted] and other friends and family [redacted] Her contacts at [redacted] are very limited. She advised that [redacted] has a very small [redacted] group that meets approximately once a month for social functions. [redacted] added that she would contact the FBI in the event she feels threatened and/or is confronted by any unusual person(s).

[redacted] advised she would not object to a polygraph if requested to do so.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
Furman University
3300 Poinsett Hwy.
Greenville, SC 29613

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on November 2, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following dates: September 22 and 24, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, furman.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f), provides:

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

288-CI-68562-29

1 - Addressee
1 - CI (288-68562) BB:bb (2)

307B301,OTH

Searched
Serialized
Indexed
Filed

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
University of Pittsburgh
600 Epsilon Drive
Pittsburgh, PA 15238

b6
b7C

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

This letter is to follow up our telephone conversation on November 2, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 18, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, unixs2.cis.pitt.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f), provides:

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

1 - Addressee
1 - CI (288-CI-68562) BB:bb (2)

288-CI-68562-30
Searched
Serialized
Indexed
Filed

30TBB02.0TH

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
Harvard University
Network Services Division
Office for Information Technology
~~10 Ware Street~~ 1 Oxford St.
Cambridge, MA 02138

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on October 30, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following dates: September 22 and 24, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, jsbach.harvard.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-31

For ease of reference, Title 18, U.S.C., 2703(f), provides:

Searched
Serialized
Indexed
Filed

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service,

1 - Addressee
(1) - CI (288-CI-68562) BB:bb (2)

307 bb 03.04h

upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
Bryn Mawr College
101 North Merion Ave.
Bryn Mawr, PA 19010-2899

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on October 30, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 23, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, serendip.brynmawr.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f) provides:

288-CI-68562-32
Searched
Serialized
Indexed
Filed

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

1 - Addressee
1 - CI (288-CI-68562) BB:bb (2)

307b04.ltr

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
Florida Institute of Technology (FIT-DOM)
150 West University Blvd.
Melbourne, FL 32901

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on October 30, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 22, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, sunmlb.new.fit.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-33

For ease of reference, Title 18, U.S.C., 2703(f), provides:

Searched
Serialized
Indexed
Filed

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

1 - Addressee
1) - CI (288-CI-68562) BB:bb (2)

307605.oth/

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
Indiana University, South Bend Campus
1700 Mishawaka Ave.
South Bend, IN 46634-7111

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): August 25 and 26, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, oit1.iusb.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f), provides:

288-CI-68562-34

Searched
Serialized
Indexed
Filed

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

1 - Addressee
1 - CI (288-CI-68562) BB:bb (2)

307506.01h

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
California Institute of Technology
Information Technology Services
014-81
Pasadena, CA 91125

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 22, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, newvortex.ama.caltech.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-35

For ease of reference, Title 18, U.S.C., 2703(f), provides:

Searched
Serialized
Indexed
Filed

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

1 - Addressee
1 - CI (288-CI-68562) BB:bb (2)

30766 07.04

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
Haverford College
Academic Computing
Haverford, PA 19041

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 23 and 24, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, io.haverford.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-36

For ease of reference, Title 18, U.S.C., 2703(f), provides:

Searched
Serialized
Indexed
Filed

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

1 - Addressee
1 - CI (288-CI-68562) BB:bb (2)

307608.oth

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted], at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
University of Texas at Austin
Office of Telecommunication Services
Services Building, Room 319
Austin, TX 78712-1024

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 22, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, net.cs.utexas.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-37

For ease of reference, Title 18, U.S.C., 2703(f), provides:

Searched
Serialized
Indexed
Filed

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary

1 - Addressee
1 - CI (288-CI-68562) BB:bb (2)

steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
Auburn University
Division of Telecommunications/ETV
Auburn University, AL 36849-5423

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 23, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, node-57-2.spidle.auburn.edu, [redacted]

b6
b7C

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-38

Searched
Serialized
Indexed
Filed

For ease of reference, Title 18, U.S.C., 2703(f), provides:

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary

1 - Addressee
1 - CI (288-CI-68562) BB:bb (2)

307 Bell South

steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

550 Main Street, Room 9000
Cincinnati, Ohio 45202
November 3, 1998

[redacted]
Duke University
407 North Building
Durham, NC 27706

RE: Notice to Preserve Evidence Under
Title 18, U.S.C., 2703(f)

Dear [redacted]

b6
b7C

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 22 and 24, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [redacted] According to our investigation, this communication originated or passed through your system, bme-www.egr.duke.edu, [redacted]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-39

For ease of reference, Title 18, U.S.C., 2703(f), provides:

Searched
Serialized
Indexed
Filed

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary

1 - Addressee
1 - CI (288-CI-68562) BB:bb (2)

307 1/2 10.01

steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) Notice of Search.- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent